

Audit

Report



YEAR 2000 COMPLIANCE OF THE
COUNTERINTELLIGENCE/HUMAN INTELLIGENCE
AUTOMATED TOOL SET

Report No. 99-124

April 6, 1999

Office of the Inspector General
Department of Defense

AQI 99-11-2140

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Year 2000 Compliance of the
Counterintelligence/Human Intelligence Automated Tool Set

B. DATE Report Downloaded From the Internet: 08/23/99

**C. Report's Point of Contact: (Name, Organization, Address, Office
Symbol, & Ph #):** OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ Preparation Date 08/23/99

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.

19990824 129

Additional Copies

To obtain additional copies of this audit report, contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932 or visit the Inspector General, DoD, home page at www.dodig.osd.mil.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or FAX (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil, or by writing to the Defense Hotline, The Pentagon, Washington, DC 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

CI/HUMINT
CHATS
PACOM
Y2K

Counterintelligence/Human Intelligence
Counterintelligence/Human Intelligence Automated Tool Set
U.S. Pacific Command
Year 2000



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202

April 6, 1999

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE (COMMAND,
CONTROL, COMMUNICATIONS, AND
INTELLIGENCE)
COMMANDER IN CHIEF, U.S. PACIFIC COMMAND
AUDITOR GENERAL, DEPARTMENT OF THE ARMY

SUBJECT: Audit Report on Year 2000 Compliance of the Counterintelligence/Human
Intelligence Automated Tool Set (Report No. 99-124)

We are providing this audit report for information and use. This is one in a series of reports being issued by the Inspector General, DoD, in accordance with an informal partnership with the Chief Information Officer, DoD, to monitor efforts to address the year 2000 computing challenge. Because this report contains no findings or recommendations, no comments were requested and none were received. Therefore, we are publishing the report in final form.

We appreciate the courtesies extended to the audit staff. Questions on the audit should be directed to Mr. Joseph P. Doyle at (703) 604-9348 (DSN 664-9348) or Mr. John Yonaitis, at (703) 604-9340 (DSN 664-9340). See Appendix B for the report distribution. The audit team members are listed inside the back cover.

A handwritten signature in black ink, reading "Robert J. Lieberman", is positioned above the printed name.

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 99-124

(Project No. 9CC-0086.04)

April 6, 1999

Year 2000 Compliance of the Counterintelligence/Human Intelligence Automated Tool Set

Executive Summary

Introduction. This is one in a series of reports being issued by the Inspector General, DoD, in accordance with an informal partnership with the Chief Information Officer, DoD, to monitor DoD efforts to address the year 2000 computing challenge. For a list of audit projects addressing the issue, see the year 2000 web page on the IGnet at <http://www.ignet.gov>.

Objectives. The overall audit objective was to assess the status of Military Department and Defense agency mission critical systems, identified by the U.S. Pacific Command and U.S. Forces Korea, as being of particular importance to them, in attaining compliance with year 2000 conversion requirements. Specifically, we reviewed the progress of each system toward year 2000 compliance, testing and integration of modifications, and contingency plans. For this report, we reviewed the Army system called Counterintelligence/Human Intelligence Automated Tool Set.

Results. The Counterintelligence/Human Intelligence Automated Tool Set hardware suite and operational software was appropriately certified year 2000 compliant in December 1998. The Counterintelligence/Human Intelligence program manager followed the Army certification process and documented the system verification, testing, interfaces, and contingency documentation before certification. The Counterintelligence/Human Intelligence program office had completed distribution of version one of the hardware suites and implementation of version two upgrades to those hardware suites was on schedule.

Management Comments. We provided a draft of this report on March 18, 1999. Because this report contains no findings or recommendations, written comments were not required, and none were received. Therefore, we are publishing the report in final form.

Table of Contents

Executive Summary

Introduction

Background	1
Objectives	2

Discussion

Year 2000 Compliance of the Counterintelligence/Human Intelligence Automated Tool Set	3
--	---

Appendixes

A. Audit Process	6
Scope	6
Methodology	7
Summary of Prior Coverage	7
B. Report Distribution	8

Background

The Executive Order, "Year 2000 Conversion," February 4, 1998, mandates that Federal agencies do what is necessary to ensure that no critical Federal program experiences disruption because of the year 2000 (Y2K) computing problem. The Executive Order also requires that the head of each agency ensure that efforts to address Y2K issues receive the highest priority.

The Assistant Secretary of Defense (Command, Control, Communications and Intelligence) is the principle staff assistant for the intelligence and counterintelligence functional areas in the Office of the Secretary of Defense. The Army has direct responsibility for ensuring the year 2000 readiness of the Counterintelligence/Human Intelligence Automated Tool Set.

The DoD Y2K Management Plan, version 2, December 1998, provides guidance for testing and certifying systems and preparing contingency plans for those systems, and stipulates the criteria that DoD Components must use to meet reporting requirements. The U.S. Army year 2000 Action Plan, revision II, June 1998, applies to all systems supported by information technology, their technical environment, and communications devices. The plan outlines the Army Y2K management strategy, provides guidance, and defines roles, responsibilities and reporting requirements.

U.S. Pacific Command. The U.S. Pacific Command (PACOM) is the largest of the nine unified commands in the DoD. The PACOM area of responsibility includes 50 percent of the earth's surface and two-thirds of the world's population. It encompasses more than 100 million square miles, stretching from the west coast of North and South America to the east coast of Africa, and from the Arctic in the North to the Antarctic in the South. It also includes Alaska and Hawaii and eight U.S. Territories. The overall mission of the PACOM is to promote peace, deter aggression, respond to crisis, and, if necessary, fight and win to advance security and stability throughout the Asian-Pacific region.

The PACOM, located at Camp Smith, Hawaii, is supported by Component commands from each service: the U.S. Army Pacific Command, U.S. Pacific Fleet Command, Marine Forces Pacific Command, and U.S. Pacific Air Forces Command. In addition, PACOM exercises combatant control over four sub-unified commands within the Pacific region. The subunified commands are the U.S. Forces Japan, U.S. Forces Korea, Alaskan Command, and Special Operations Command Pacific.

Counterintelligence/Human Intelligence Automated Tool Set System. The Counterintelligence/Human Intelligence Automated Tool Set (CHATS) is an Army managed hardware suite consisting of a processor, peripherals, and communications that are designed to meet the requirements of

Counterintelligence/Human Intelligence (CI/HUMINT) teams operating in the field. CHATS provides intelligence teams the capability to control and analyze information obtained through investigations, interrogations, and collections operations while providing automated intelligence and information management. This includes interface data handling to meet time and accuracy reporting requirements for counterintelligence/human intelligence, force protection-related decision support and operations planning and execution.

The technical testing of CHATS was performed in October 1997. The CHATS program office began fielding the hardware suites in November 1997. The compliance checklist and validation testing for the CHATS hardware suite was completed in December 1998.

Objectives

The overall objective was to assess the status of Military Department and Defense Agency mission critical systems, identified by the PACOM and U.S. Forces Korea as being of particular importance to them, in attaining compliance with year 2000 conversion requirements. Specifically, we reviewed the progress of each system towards year 2000 compliance, testing and integration of modifications, and contingency plans. For this report, we reviewed the Army system called Counterintelligence/Human Intelligence Automated Tool Set. See Appendix A for a discussion of the scope and methodology.

Year 2000 Compliance of the Counterintelligence/Human Intelligence Automated Tool Set

The Counterintelligence/Human Intelligence Automated Tool Set (CHATS) hardware suite was appropriately certified as year 2000 compliant in December 1998. The Counterintelligence/Human Intelligence program manager followed the Army certification process and documented the verification, testing, interfaces, and contingency documentation before certification of the CHATS hardware suite. The Counterintelligence/Human Intelligence program office had completed distribution of version one of the hardware suites, and implementation of version two upgrades to those hardware suites was on schedule. As a result, the Army has minimized the risk of year 2000 failure of the CHATS hardware suite.

Y2K Compliance of CHATS

The CI/HUMINT program office, a part of the Army Intelligence Fusion Project office, is responsible for the CHATS system with oversight from Headquarters, Department of the Army. The U.S. Army White Sands Missile Range Electronic Proving Ground at Fort Huachuca, Arizona, conducted the year 2000 operational tests of the CHATS systems and their command, control, and communication systems division certified the CHATS system year 2000 compliant on December 22, 1998.

Y2K Tests of the CHATS. There were three distinct operational tests of CHATS performed. The operational tests included the following categories.

1. Manual entry of date changeovers to identify potential problems. These tests included system date/time rollover, date entry and database saves within selected Defense Counterintelligence Threat Data System Store/Forward reports, and data entry in CI/HUMINT utilities.
2. Attempted manual entry of improper dates.
3. Automated year 2000 verification.

Results of Y2K Testing. The operational tests of the CHATS hardware suite was made using the installed Counterintelligence/Human Intelligence All Source Integration System version 1.5.3 operational software in November 1998. CHATS passed all elements of the three operational tests and was determined to be Y2K compliant.

Subsequent Versions of CHATS. Subsequent versions of CHATS are under development. The program office is upgrading CHATS version one and developing CHATS version two. CHATS version two will be enhanced to include a:

- single channel ground and airborne radio system communication interface,
- precision lightweight global positioning system receiver interface,
- secure data communications device, and
- zip drive data storage device.

In addition, the CHATS program management office executed a memorandum of agreement with the product managers of the All Source Analysis System-Software and Migration Defense Intelligence Threat Data System that will allow the CHATS version two hardware suite to send and receive, not just send as in version one, information beyond the year 2000.

The improvements will fill the additional requirements identified by the Army and the Marine Corps. The CHATS version 2 fielding is scheduled to begin June 1999.

Contingency Management Plan

The CI/HUMINT program management office identified risks to the CHATS hardware suite and developed a series of five contingency management plans aimed at correcting potential problems that could occur. The five contingencies cover completion of renovations, fielding the hardware suite with defects, message failures, noncompliant hardware failures, and Y2K certification testing failure. The plans listed specific risks, the probability of occurrence and the corrective action to be taken.

Conclusion

The CI/HUMINT program management office complied with DoD and Army guidance in processing the CHATS system Y2K certification. The CHATS

hardware suite has been determined to be Y2K compliant. The CHATS program office is on schedule to conduct the operational testing of version two and fielding that hardware suite; therefore, we have no recommendations.

Appendix A. Audit Process

This is one in a series of reports being issued by the Inspector General, DoD, in accordance with an informal partnership with the Chief Information Officer, DoD, to monitor DoD efforts to address the year 2000 computing challenge. For a list of audit projects addressing the issue, see the Y2K web page on the IGnet at <http://www.ignet.gov>.

Scope

We reviewed and evaluated the Counterintelligence/Human Intelligence Automated Tool Set (CHATS) hardware suite. We visited the CI/HUMINT program management office responsible for CHATS and met with CHATS officials to obtain the year 2000 status of the mission critical system. During our meetings, we obtained data pertaining to the CHATS program.

DoD-wide Corporate Level Government Performance and Results Act Goals. In response to the Government Performance Results Act, the Department of Defense has established 6 DoD-wide corporate level performance objectives and 14 goals for meeting these objectives. This report pertains to achievement of the following objectives and goals.

- **Objective:** Prepare now for an uncertain future. **Goal:** Pursue a focused modernization effort that maintains U.S. qualitative superiority in key war fighting capabilities. (DoD-3)

DoD Functional Area Reform Goals. Most major DoD functional areas have also established performance improvement reform objectives and goals. This report pertains to achievement of the following functional area objectives and goals.

- **Information Technology Management Functional Area.**
Objective: Become a mission partner.
Goal: Serve mission information users as customers. (ITM-1.2)
- **Information Technology Management Functional Area.**
Objective: Provide services that satisfy customer information needs.
Goal: Modernize and integrate DoD information infrastructure. (ITM 2.2)
- **Information Technology Management Functional Area.**
Objective: Provide services that satisfy customer information needs.
Goal: Upgrade technology base. (ITM-2.3)

General Accounting Office High-Risk Area. In its identification of high-risk areas, the General Accounting Office has specifically designated risk in resolution of the Y2K problem as high. This report provides coverage of that problem and the overall Information Management and Technology high-risk area.

Methodology

Audit Type, Dates, and Standard. We performed this program audit in March 1999 in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD. We did not use computer-processed data to perform this audit.

Contacts During the Audit. We visited or contacted individuals and organizations within DoD and SYTEX, Inc. Further details are available upon request.

Management Control Program. We did not review the management control program related to the overall audit objective because DoD recognized the Y2K issue as a material management control weakness area in the FY 1997 Annual Statement of Assurance.

Summary of Prior Coverage

The General Accounting Office and the Inspector General, DoD, have conducted multiple reviews related to the Y2K issues. General Accounting Office reports can be accessed over the internet at <http://www.gao.gov>. Inspector General, DoD, reports can be accessed over the internet at <http://www.dodig.osd.mil>.

Appendix B. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition and Technology
Director, Defense Logistics Studies Information Exchange
Under Secretary of Defense (Comptroller)
Deputy Chief Financial Officer
Deputy Comptroller (Program/Budget)
Under Secretary of Defense for Personnel and Readiness
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
Deputy Assistant Secretary of Defense (Command, Control, Communications,
Intelligence, Surveillance, Reconnaissance, and Space Systems)
Deputy Chief Information Officer and Deputy Assistant Secretary of Defense (Chief
Information Officer Policy and Implementation)
Principal Deputy - Y2K
Assistant Secretary of Defense (Public Affairs)

Joint Staff

Director, Joint Staff

Department of the Army

Assistant Secretary of the Army (Financial Management and Comptroller)
Auditor General, Department of the Army
Chief Information Officer, Army
Army Intelligence Fusion Project Office

Department of the Navy

Assistant Secretary of the Navy (Financial Management and Comptroller)
Auditor General, Department of the Navy
Chief Information Officer, Navy

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Auditor General, Department of the Air Force
Chief Information Officer, Air Force

Unified Command

Commander in Chief, U.S. European Command
Commander in Chief, U.S. Pacific Command
Commander in Chief, U.S. Atlantic Command
Commander in Chief, U.S. Central Command
Commander in Chief, U.S. Special Operations Command

Other Defense Organizations

Director, Defense Information Systems Agency
Chief Information Officer, Defense Information Systems Agency
Inspector General, Defense Information Systems Agency
United Kingdom Liaison Officer, Defense Information Systems Agency
Director, National Security Agency
Inspector General, National Security Agency
Inspector General, Defense Intelligence Agency
Inspector General, National Imagery and Mapping Agency
Inspector General, National Reconnaissance Office

Non-Defense Federal Organizations and Individuals

Office of Management and Budget
General Accounting Office
National Security and International Affairs Division,
Technical Information Center,
Accounting and Information Management Division
Director, Defense Information and Financial Management Systems

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
Senate Special Committee on the Year 2000 Technology Problem
Senate Committee on Intelligence
House Committee on Appropriations
House Subcommittee on National Security, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Management, Information, and Technology,
Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, and International
Relations, Committee on Government Reform
House Subcommittee on Technology, Committee on Science
House Permanent Select Committee on Intelligence

Audit Team Members

The Contract Management Directorate, Office of the Assistant Inspector General
for Auditing, DoD, prepared this report

Paul J. Granetto
Joseph P. Doyle
John Yonaitis
Gopal Jain
Michael Guagliano